Information Theoretically Secure Hypothesis Test for Temporally Unstructured Quantum Computing

How Do I Know If You Have A Quantum Computer

Daniel Mills[1], Anna Pappa[12], Theodoros Kapourniotis[13], and Elham Kashefi[14]

QPL, July 4, 2017

[1]School of Informatics, The University of Edinburgh

[2]Department of Physics, University College London

[3]Department of Physics, University of Warwick

[4]LIP6, CNRS, Pierre et Marie Curie University

This Presentation

Introduction

Introduction

Introduction

Introduction


I think I'll buy a quantum computer
Are you sure this seller has one?
Well I can't check the computations with my computer
Is he even sure he has one?
You're always so sceptical. I'll send him a Hypothesis test

A well designed *Hypothesis test* should allow:

Introduction

A well designed *Hypothesis test* should allow:

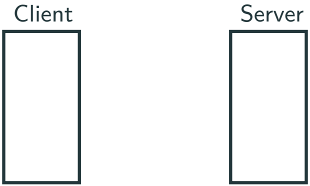
- A Client to ensure a malicious Server is capable of quantum computations.

Introduction

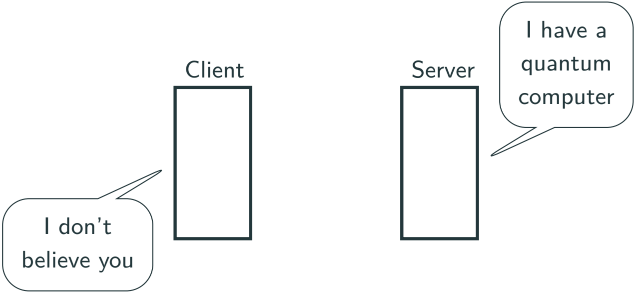
A well designed *Hypothesis test* should allow:

- A Client to ensure a malicious Server is capable of quantum computations.
- An engineer to check their machine is capable of quantum computations.

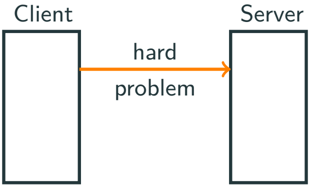
A Proposal



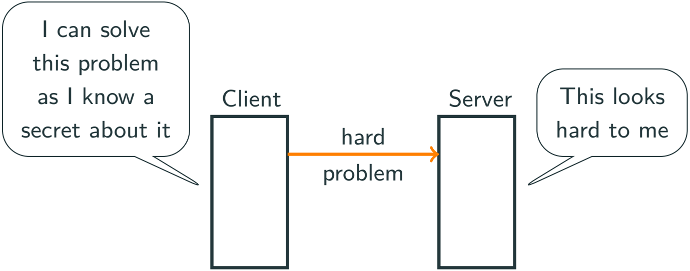
A Proposal



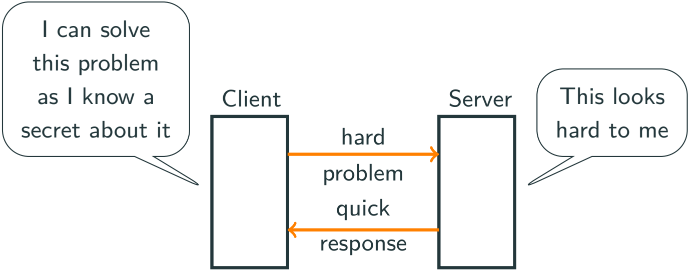
A Proposal



A Proposal

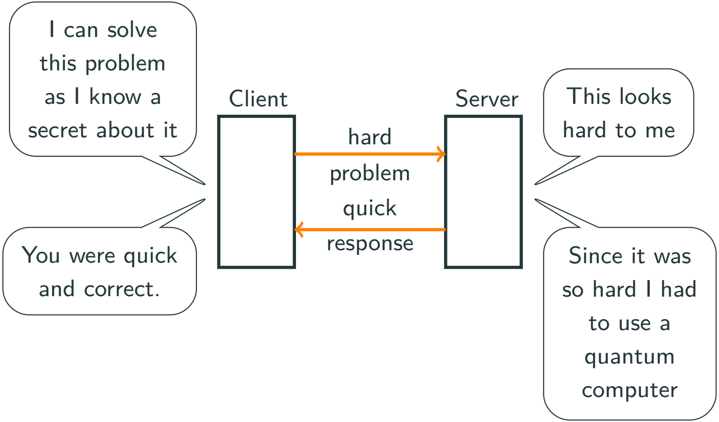

I can solve this problem as I know a secret about it
Client
hard problem
Server
This looks hard to me

A Proposal

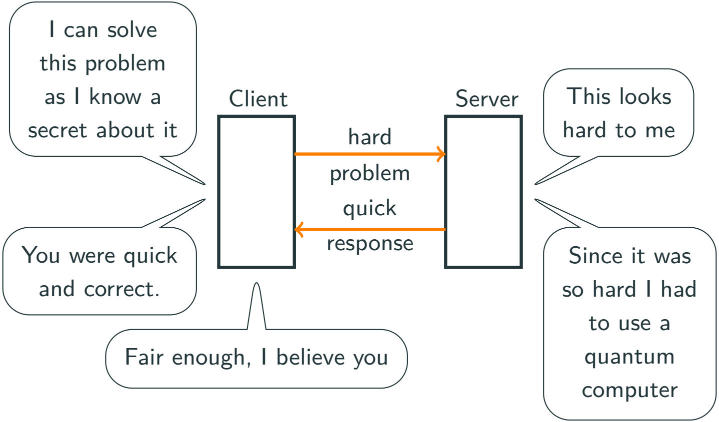


I can solve this problem as I know a secret about it
Client
Server
This looks hard to me
hard problem
quick response

A Proposal


I can solve this problem as I know a secret about it
Client
Server
This looks hard to me
hard problem
quick response
You were quick and correct.
Since it was so hard I had to use a quantum computer

A Proposal


I can solve this problem as I know a secret about it
Client
Server
This looks hard to me
hard problem
quick response
You were quick and correct.
Since it was so hard I had to use a quantum computer
Fair enough, I believe you

A Proposal

So three conditions for a successful hypothesis test might be:

A Proposal

So three conditions for a successful hypothesis test might be:

- The Server must complete a hard computations
    - This means it is capable of computations from some class

A Proposal

So three conditions for a successful hypothesis test might be:

- The Server must complete a hard computations
  - This means it is capable of computations from some class
- The Client knows a secret property allowing them to check the outcome
  - Must be sure that this does not add structure to the problem which the Server can use

A Proposal

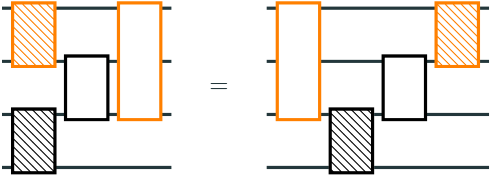
So three conditions for a successful hypothesis test might be:

- The Server must complete a hard computations
  - This means it is capable of computations from some class
- The Client knows a secret property allowing them to check the outcome
  - Must be sure that this does not add structure to the problem which the Server can use
- The Client hides the secret property

IQP in MBQC

Instantaneous Quantum Polytime Machine [Shepherd and Bremner, 2009]

Commuting gates:



In particular:

$$\exp\left\{ i\theta \bigotimes_{i:q_i=1} X_i \right\}$$

where $q \in \{0,1\}^{n_p}$, $\theta \in [0, 2\pi]$.

Instantaneous Quantum Polytime Machine [Shepherd and Bremner, 2009]

$$\exp\left\{ i\theta \bigotimes_{i:q_i=1} X_i \right\}$$

An IQP program may consist of many of these gates, and so many different q. Hence we may represent the whole computation by, for example:

$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

where, in this case, we have two gates defined by $q = (101)$ and $q = (010)$.

The input is $|0^{n_p}\rangle$ and the output is the resulting state measured in the computational basis.

Instantaneous Quantum Polytime Machine [Shepherd and Bremner, 2009]

$$\exp\left\{ i\theta \bigotimes_{i:q_i=1} X_i \right\}$$

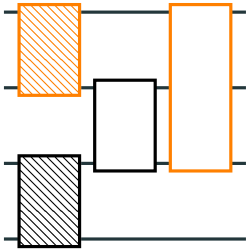
An IQP program may consist of many of these gates, and so many different q. Hence we may represent the whole computation by, for example:

$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

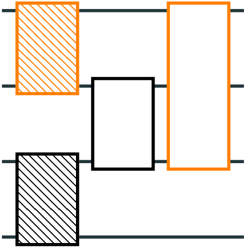
where, in this case, we have two gates defined by $q = (101)$ and $q = (010)$.

The input is $|0^{n_p}\rangle$ and the output is the resulting state measured in the computational basis.

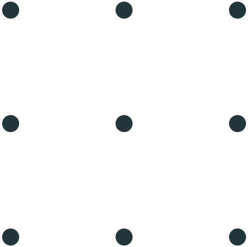
Thought not to be classically simulateable [Bremner et al., 2010]



Measurement Based Quantum Computing [Raussendorf and Briegel, 2001]

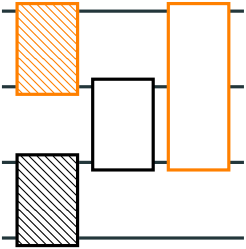


vs

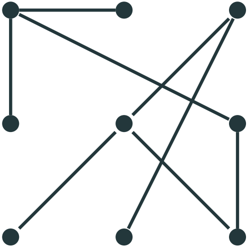


$\bigotimes |+\rangle$

Measurement Based Quantum Computing [Raussendorf and Briegel, 2001]

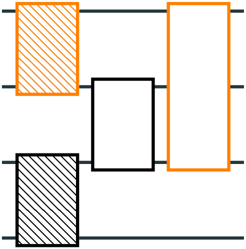


vs

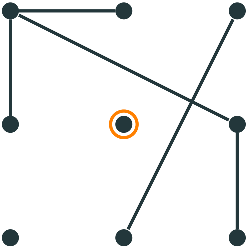


$cZ \ldots cZ \bigotimes |+\rangle$

Measurement Based Quantum Computing [Raussendorf and Briegel, 2001]

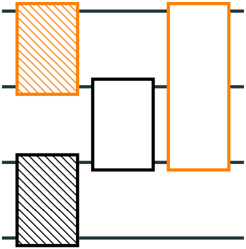


vs

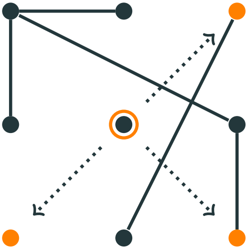


$$|m\rangle \langle m| \, cZ...cZ \bigotimes |+\rangle$$

Measurement Based Quantum Computing [Raussendorf and Briegel, 2001]

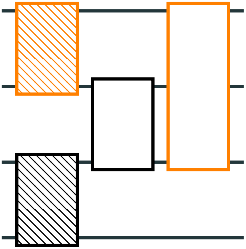


vs

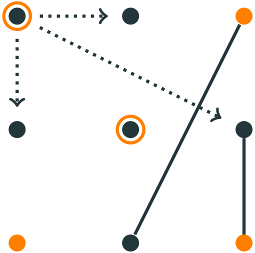


$C \ldots CcZ \ldots cZ \bigotimes |+\rangle$

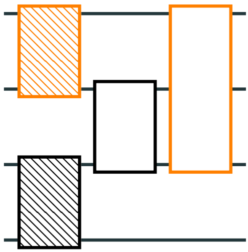
Measurement Based Quantum Computing [Raussendorf and Briegel, 2001]



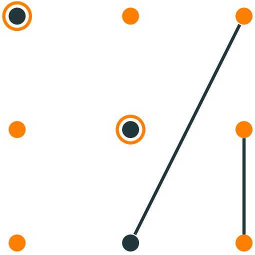
vs



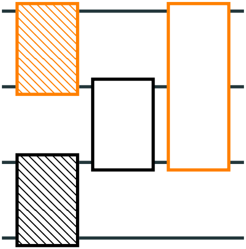
Measurement Based Quantum Computing [Raussendorf and Briegel, 2001]



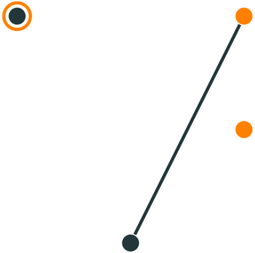
vs



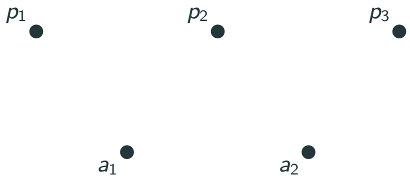
Measurement Based Quantum Computing [Raussendorf and Briegel, 2001]



vs

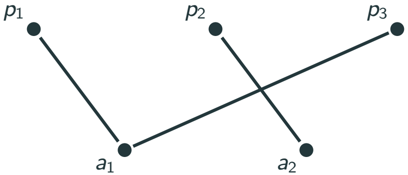


IQP in MBQC



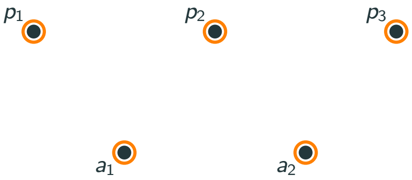
$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

IQP in MBQC



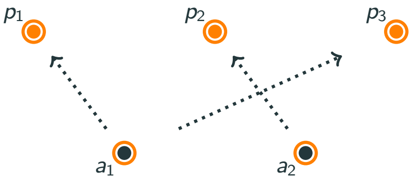
$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

IQP in MBQC



$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

IQP in MBQC



$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

IQP in MBQC

$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Blind IQP

Bridge and Break [Fitzsimons and Kashefi, 2012]

$cZ_{1,2}cZ_{2,3} \, |0/1\rangle \otimes |\phi\rangle$

Bridge and Break [Fitzsimons and Kashefi, 2012]

$$Z_1^{0/1} Z_3^{0/1} |0/1\rangle \otimes |\phi\rangle$$

Bridge and Break [Fitzsimons and Kashefi, 2012]

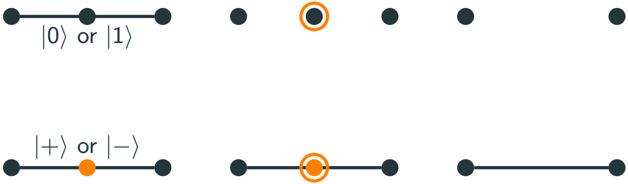
Bridge and Break [Fitzsimons and Kashefi, 2012]

$cZ_{1,2}cZ_{2,3}\,|+/-\rangle \otimes |\phi\rangle$

Bridge and Break [Fitzsimons and Kashefi, 2012]

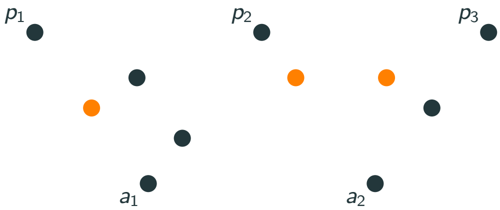
$$cZ_{1,2}cZ_{2,3}\,|+/-\rangle \otimes |\phi\rangle$$

Bridge and Break [Fitzsimons and Kashefi, 2012]

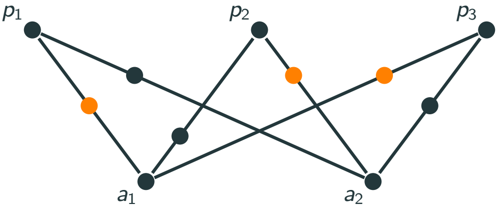


$S_1^{f(+/-,s)} S_3^{f(+/-,s)} Z_{1,3} |\phi\rangle$

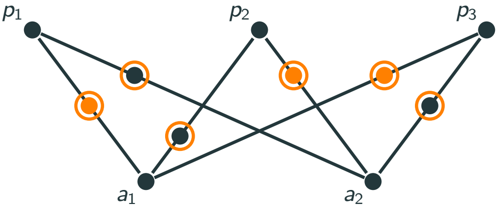
IQP By Bridge and Break



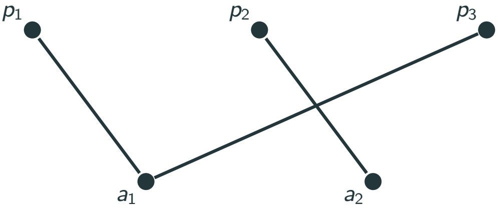
IQP By Bridge and Break



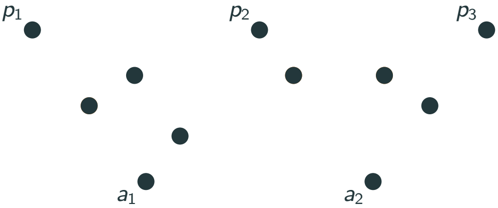
IQP By Bridge and Break



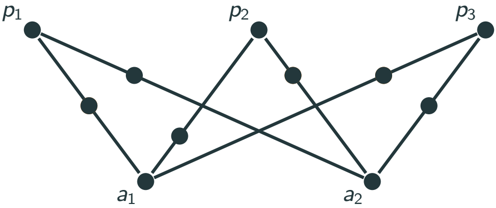
IQP By Bridge and Break



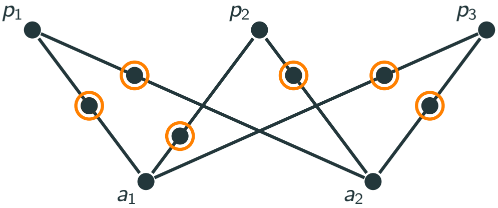
IQP By Bridge and Break



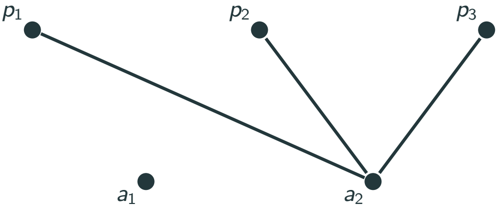
IQP By Bridge and Break



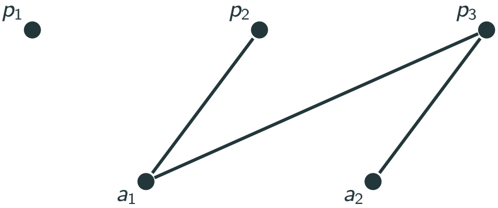
IQP By Bridge and Break



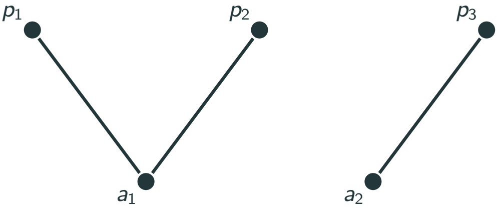
IQP By Bridge and Break



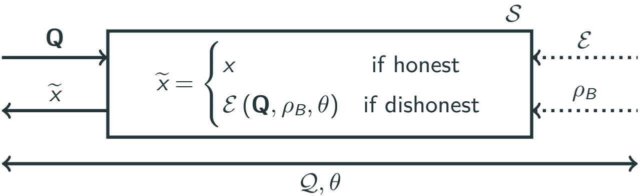
IQP By Bridge and Break



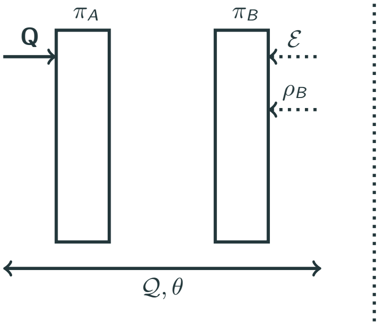
IQP By Bridge and Break



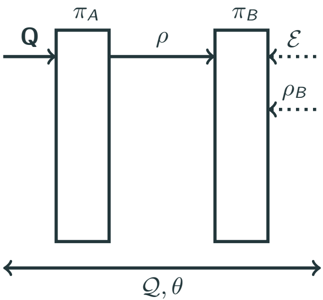
Blind IQP Ideal Resource [Dunjko et al., 2014]

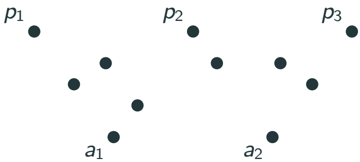


Blind IQP Real Resource

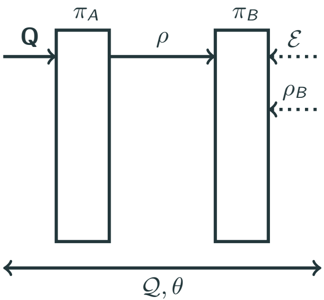


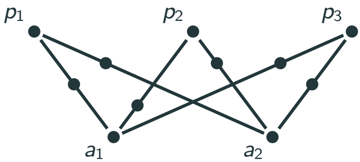
Blind IQP Real Resource



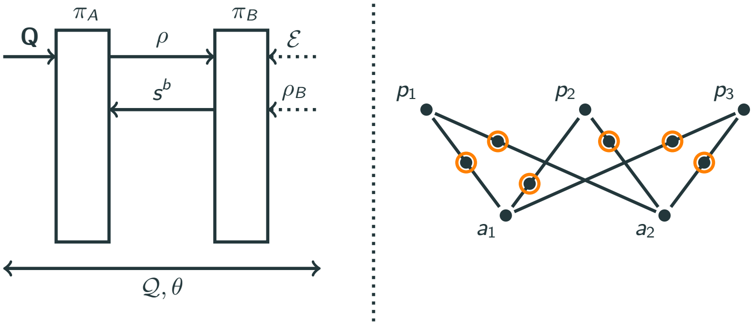


Blind IQP Real Resource

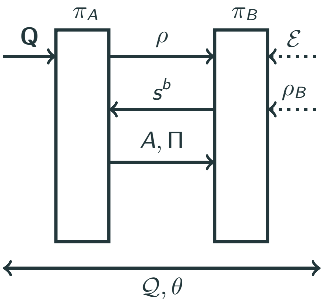


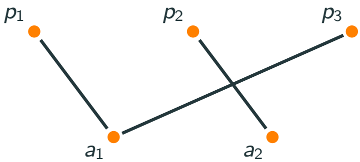


Blind IQP Real Resource

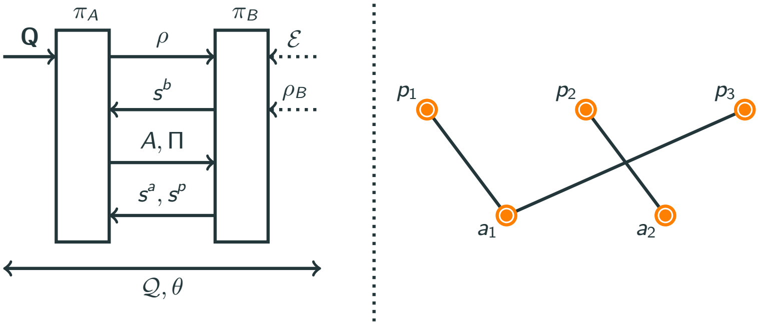


Blind IQP Real Resource

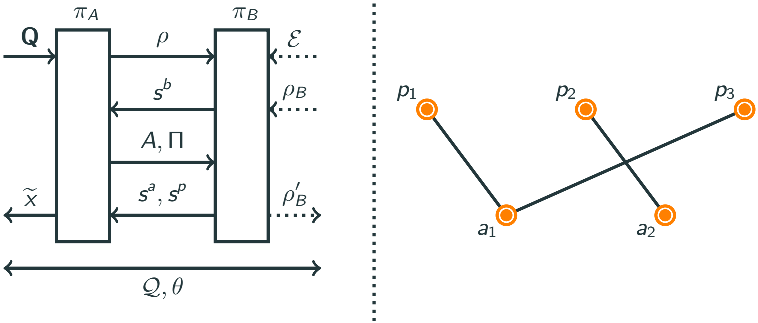




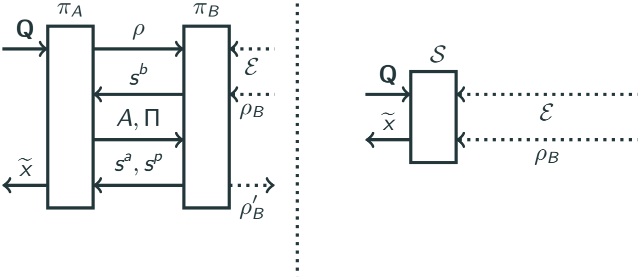
Blind IQP Real Resource



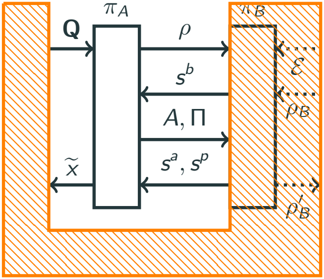
Blind IQP Real Resource

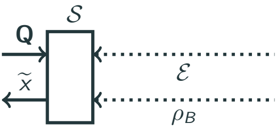


Blind IQP Real vs Ideal Resource

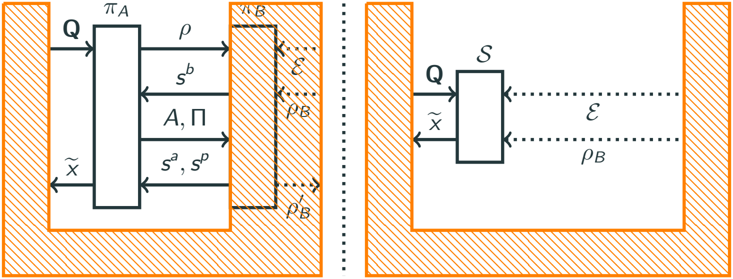


Blind IQP Real vs Ideal Resource

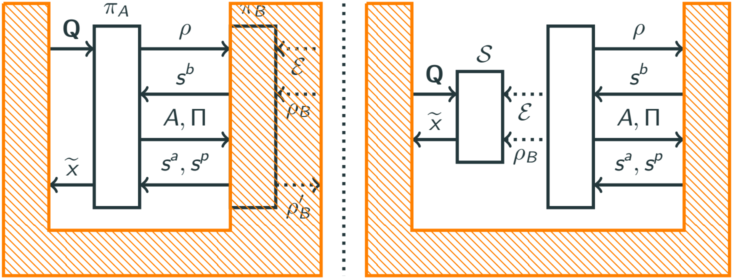




Blind IQP Real vs Ideal Resource



Blind IQP Real vs Ideal Resource



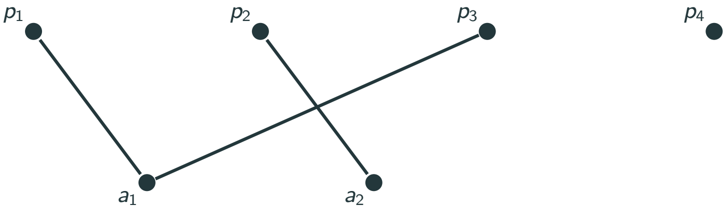
The Hypothesis Test

Bias of a random variable, $X \in \{0,1\}^{n_p}$, in a direction $s \in \{0,1\}^{n_p}$.

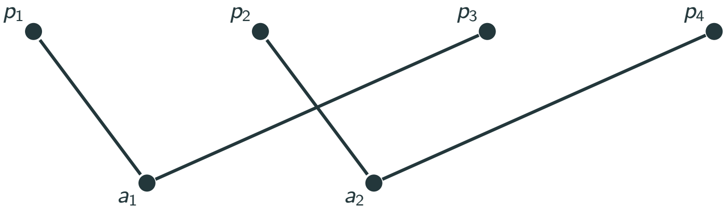
$$\mathbb{P}\left(X \cdot s^T = 0\right) = \mathit{Bias}(X, s)$$

Can be easily calculated, for some special IQP computations (depending on s), if one knows s [Shepherd and Bremner, 2009].

Hypothesis Test

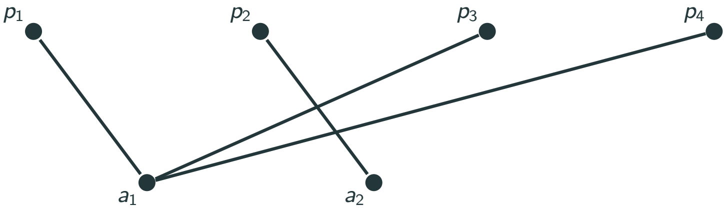


Hypothesis Test



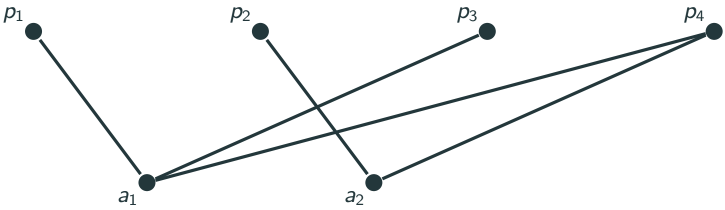
$$Bias(X, s_1) = p$$

Hypothesis Test



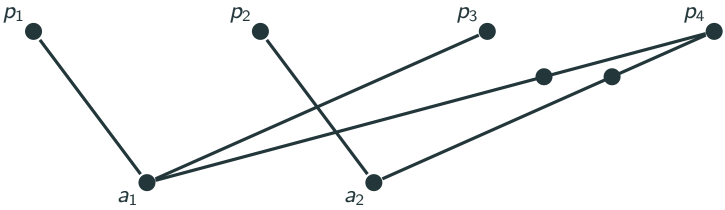
$$Bias(X, s_2) = p$$

Hypothesis Test

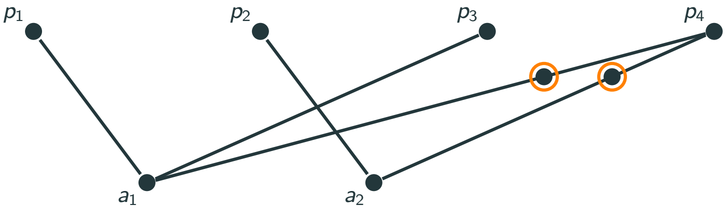


$$Bias(X, s_3) = p$$

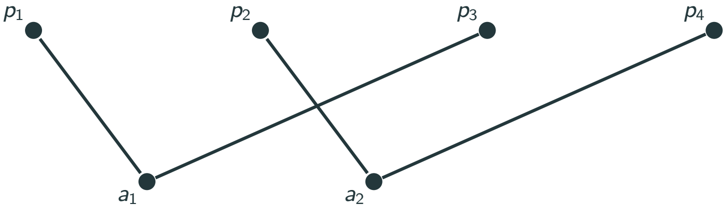
Hypothesis Test



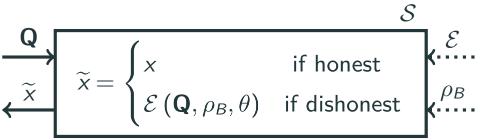
Hypothesis Test



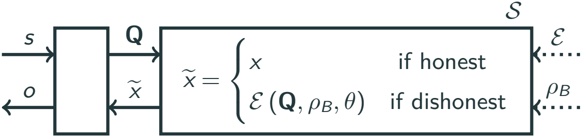
Hypothesis Test



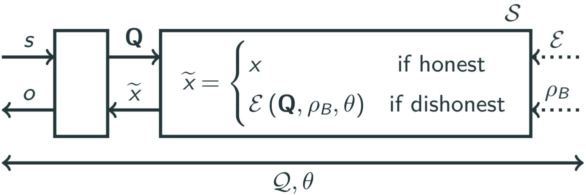
Blind IQP Ideal Resource Used in Hypothesis Test



Blind IQP Ideal Resource Used in Hypothesis Test

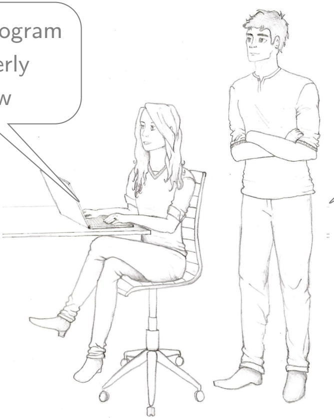


Blind IQP Ideal Resource Used in Hypothesis Test



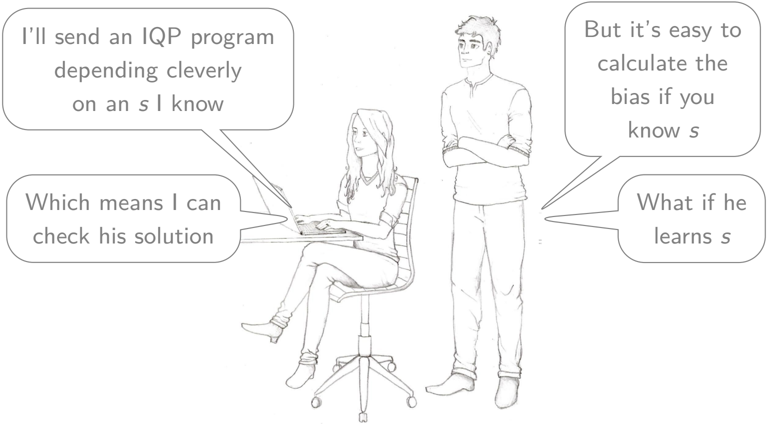
The Hypothesis Test Outline

I'll send an IQP program depending cleverly on an s I know

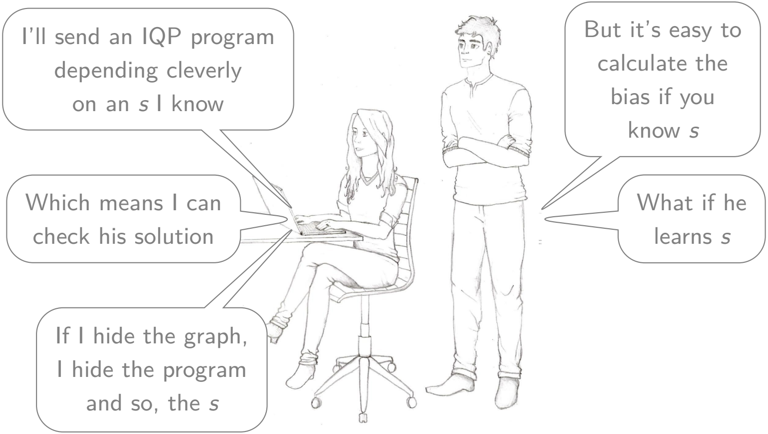


But it's easy to calculate the bias if you know s

The Hypothesis Test Outline



The Hypothesis Test Outline



The Hypothesis Test Outline

I'll send an IQP program depending cleverly on an s I know

Which means I can check his solution

If I hide the graph, I hide the program and so, the s

But it's easy to calculate the bias if you know s

What if he learns s

Seems legit

Three conditions for a successful hypothesis test:

The Hypothesis Test Outline

Three conditions for a successful hypothesis test:

- The Server must complete a hard computations
  - Computation bias calculation is hard

Three conditions for a successful hypothesis test:

- The Server must complete a hard computations
    - Computation bias calculation is hard
- The Client knows a secret property allowing them to check the outcome
    - The Client knows the direction s

The Hypothesis Test Outline

Three conditions for a successful hypothesis test:

- The Server must complete a hard computations
  - Computation bias calculation is hard
- The Client knows a secret property allowing them to check the outcome
  - The Client knows the direction s
- The Server hides the secret property
  - Using blind IQP

Closing Remarks

Conclusion:

- Blind IQP computation
- Can hide computable computation in hard one
- Might allow demonstration of quantum supremacy in early devices

Conclusion:

- Blind IQP computation
- Can hide computable computation in hard one
- Might allow demonstration of quantum supremacy in early devices

Future work:

- Hypothesis test for other devices
- Tolerance to noise
- Small implementation

Closing Remarks

Conclusion:

- Blind IQP computation
- Can hide computable computation in hard one
- Might allow demonstration of quantum supremacy in early devices

Future work:

- Hypothesis test for other devices
- Tolerance to noise
- Small implementation

The paper:

arxiv.org/abs/1704.01998

[Bremner et al., 2010] Bremner, M. J., Jozsa, R., and Shepherd, D. J. (2010). **Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy.** In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, page rspa20100301. The Royal Society.

[Dunjko et al., 2014] Dunjko, V., Fitzsimons, J. F., Portmann, C., and Renner, R. (2014). **Composable security of delegated quantum computation.** In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 406–425. Springer.

[Fitzsimons and Kashefi, 2012] Fitzsimons, J. F. and Kashefi, E. (2012). **Unconditionally verifiable blind computation.** *arXiv preprint arXiv:1203.5217*.

Bibliography II

[Raussendorf and Briegel, 2001] Raussendorf, R. and Briegel, H. J. (2001).
A one-way quantum computer.
Physical Review Letters, 86(22):5188.

[Shepherd and Bremner, 2009] Shepherd, D. and Bremner, M. J. (2009).
Temporally unstructured quantum computation.
In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 465, pages 1413–1439. The Royal Society.

Thanks to:

EPSRC
Engineering and Physical Sciences Research Council

EPSRC Centre for Doctoral Training in Pervasive Parallelism

THE UNIVERSITY of EDINBURGH
informatics